Procedure No. 2205.10: Information Technology Standards
Reference: Policy 2205
Effective Date: 12/28/04
Prior Issue: N/A

Purpose:

The Arizona Department of Juvenile Corrections (ADJC) Management of Information Services (MIS) define standards to be met by all information technology equipment owned and/or operated by ADJC located outside ADJC's corporate Internet firewalls. These standards are designed to minimize the potential exposure to ADJC from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of ADJC resources.

This procedure defines the following standards:

- Ownership responsibility;
- Secure configuration requirements;
- Operational requirements;
- Change control requirement.

Rules:

1. The scope of this procedure covers the following:
   a. All equipment or devices deployed in a Demilitarized Zone (DMZ) owned and/or operated by ADJC (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by ADJC;
   b. Any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the ADJC domain or appears to be owned by ADJC.

2. **MIS** shall configure all new equipment which falls under the scope of this procedure according to the referenced configuration documents, unless a waiver is obtained from Government Information Technology Administration (GITA). All existing and future equipment deployed on ADJC's un-trusted networks shall comply with this policy.

3. **MIS** shall ensure services that are provided through the Internet (Web-enabled applications, FTP, Mail, DNS, etc.) be deployed on a Demilitarized Zone (DMZ) or proxied from the DMZ without authentication.

4. **SUPPORT GROUPS** shall administer equipment and applications within the scope of this procedure and which are approved by MIS for DMZ system, application, and/or network management. **SUPPORT GROUPS** will be responsible for the following:
   a. Equipment shall be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
      i. Host contacts and location;
      ii. Hardware and operating system/version;
      iii. Main functions and applications;
      iv. Password groups for privileged passwords.
   b. Network interfaces shall have appropriate Domain Name Server records (minimum of A and PTR records);
   c. Password groups shall be maintained in accordance with the corporate wide password management system/process;
   d. Immediate access to equipment and system logs shall be granted to members of MIS upon demand, per the *Audit Procedure;*
   e. Changes to existing equipment and deployment of new equipment shall follow and corporate governess or change management processes/procedures.

5. To verify compliance with this policy, **MIS** shall periodically audit DMZ equipment per the *Audit Procedure*.

6. MIS shall approve hardware, operating systems, services and applications as part of the pre-deployment review phase. **MIS** shall ensure that all equipment comply with the following configuration standards:
   a. Operating system configuration shall be done according to the secure host and router installation and configuration standards;
   b. All patches/hot-fixes recommended by the equipment vendor and MIS shall be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups shall have processes in place to stay current on appropriate patches/hot fixes through automated processes;
   c. Services and applications not serving business requirements shall be disabled.
   d. Trust relationships between systems may only be introduced according to business requirements, shall be documented, and shall be approved by MIS;
   e. Services and applications not for general access shall be restricted by access control lists.
   f. Insecure services or protocols (as determined by MIS) shall be replaced with more secure equivalents whenever such exist;
   g. Remote administration shall be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) shall be used for all access levels;
   h. All host content updates shall occur over secure channels;
   i. Security-related events shall be logged and audit trails saved to MIS approved logs. Security-related events include (but are not limited to) the following:
      i. User login failures;
      ii. Failure to obtain privileged access;
      iii. Access policy violations.

7. **MIS** shall address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

8. Equipment Outsourced to External Service Providers**:** **MIS** shall ensure that the responsibility for the security of the equipment and escalation procedures deployed by external service providers is clarified and documented in the contract with the service provider and security contacts. **CONTRACTING DEPARTMENTS** are responsible for third party compliance with this procedure.

9. Firewall Technology**:** **MIS** shall employ firewall technology at the edge of an agency’s network, including the Internet Gateway, to protect sensitive internal information assets and infrastructure from unauthorized access. **MIS** shall route external traffic through secure gateways, such as firewalls.

10. Intrusion Detection**:** **MIS** shall incorporate intrusion detection mechanisms into all servers connected to WANs and to all internetworking devices that serve as gateways between WAN network segments; i.e. Server Farm Network, Wireless Network, VPN Network.

11. Enforcement: Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract off the State approved vendors’ lists.

Effective Date:	**Approved by Process Owner:**	**Review Date:**	**Reviewed By:**